Exhibit 12

The New York Times https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html

D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump

By David E. Sanger and Nick Corasaniti

June 14, 2016

WASHINGTON — Two groups of Russian hackers, working for competing government intelligence agencies, penetrated computer systems of the Democratic National Committee and gained access to emails, chats and a trove of opposition research against Donald J. Trump, according to the party and a cybersecurity firm.

One group placed espionage software on the committee's computer servers last summer, giving it unimpeded access to communications for about a year. The committee called in CrowdStrike, a cybersecurity firm, early last month after the Democratic Party began to suspect an intrusion.

A senior government official said Hillary Clinton's presidential campaign, based in Brooklyn, also appeared to have been targeted, but it was not clear whether it lost any data. The breach at the Democratic committee was first reported on Tuesday by The Washington Post.

The committee's systems appeared to have had standard cyberprotections, which are no challenge for determined state-sponsored hacking groups. The attackers were expelled last weekend with CrowdStrike's help, the committee said. It did not provide a detailed account of what had been copied from the systems, and it may never know.

The connection to Russia may be explained simply by the global fascination with the presidential campaign and the mystery surrounding Mr. Trump, who has not been a major subject of foreign intelligence collection. But it also recalls a subplot to the race: Paul Manafort, Mr. Trump's campaign chairman, previously advised pro-Russian politicians in Ukraine and other parts of Eastern Europe, including former President Viktor F. Yanukovych of Ukraine.

Opposition research itself is not all that valuable to a foreign government, but it can point to a candidate's vulnerabilities. To a foreign government fascinated by an American election, any intelligence a campaign develops on an opponent could be exploited.

Dmitri Alperovitch, a co-founder of CrowdStrike, said he believed that the group that first hacked the committee's servers — a group his firm had named Cozy Bear long before the breach — appeared to be the same that downloaded communications in recent years from unclassified email systems used by the State Department and the White House.

In 2014 and 2015, the effort to clean the State Department systems after those intrusions resulted in several shutdowns, some in the midst of delicate negotiations with Iran. The administration has never confirmed that the Russian government was behind those intrusions, but it has briefed officials on the details in classified sessions.

"These are incredibly sophisticated groups," Mr. Alperovitch said. "They covered their tracks well. It wasn't until the second group came in," stealing the opposition research on Mr. Trump, "that their presence was detected."

The second group, named Fancy Bear, which appeared to have attacked in April, is believed to be operated by the G.R.U., the military intelligence service. Its past targets have included military and aerospace organizations from the United States, Europe, Canada, Japan and South Korea.

CrowdStrike concluded that neither Russian group knew the other was attacking the same organization. "One would steal a password, and the next day the other group would steal the same password," Mr. Alperovitch said.

Mrs. Clinton said on Telemundo that she had learned of the breach only after news outlets reported it. She called it "troubling," but said she was unsure about the hackers' goals.

"Now, why?" she asked. "We don't know yet. So far as we know, my campaign has not been hacked into, and we're obviously looking hard at that. But cybersecurity will be an issue that I will be absolutely focused on as president. Because whether it's Russia, or China, Iran or North Korea, more and more countries are using hacking to steal our information, to use it to their advantage, and we can't let that go on."

The Office of Personnel Management, whose files on about 22 million Americans with security clearances or applications for them were breached by Chinese hackers, is still trying to assess the damage first detected last year.

The Democratic committee avoided any discussion of its vulnerabilities.

"The security of our system is critical to our operation and to the confidence of the campaigns and state parties we work with," said Representative Debbie Wasserman Schultz of Florida, the Democratic national chairwoman. "When we discovered the intrusion, we treated this like the serious incident it is and reached out to CrowdStrike immediately. Our team moved as quickly as possible to kick out the intruders and secure our network.”

The party did not say how it came to suspect the intrusion.

Cyberattacks by foreign governments are a constant threat to political campaigns. Because campaign operations are temporary, they often do not invest heavily in the kind of security that financial institutions, large companies and government agencies spend millions or billions of dollars on each year.

And because campaigns are so far-flung, with volunteers connecting through laptops and cellphones, they are particularly vulnerable. In 2008, hackers traced to the Chinese government infiltrated the campaigns of both Barack Obama and John McCain.

“It should come as no surprise to anyone that political parties are high-profile targets for foreign intelligence gathering,” Representative Jim Langevin, a Rhode Island Democrat who has been deeply involved in cyberissues, said in a statement. “Nonetheless, it is disconcerting that two independent operations were able to penetrate the D.N.C., one of which was able to stay embedded for nearly a year.”